FIG. 1

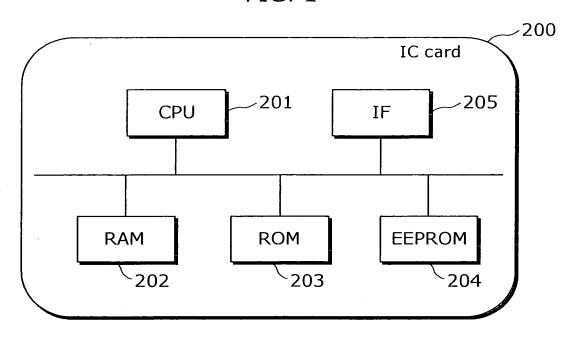


FIG. 2

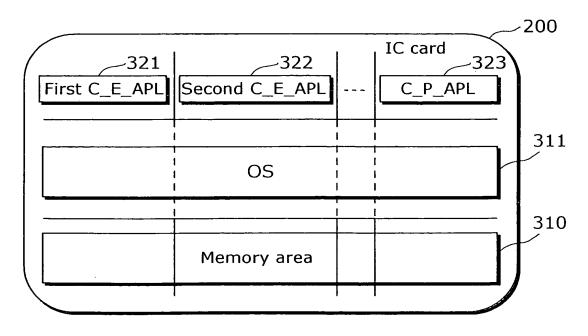


FIG. 3

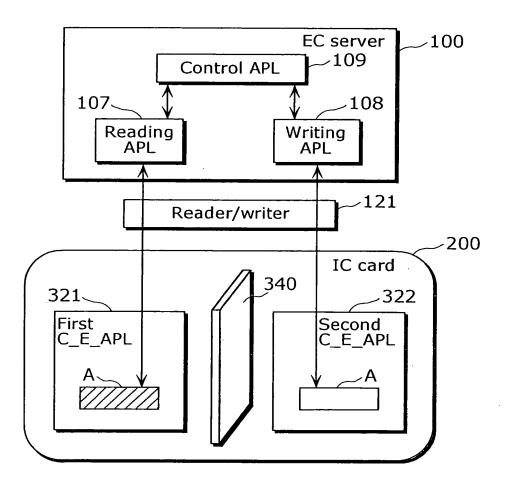


FIG. 4

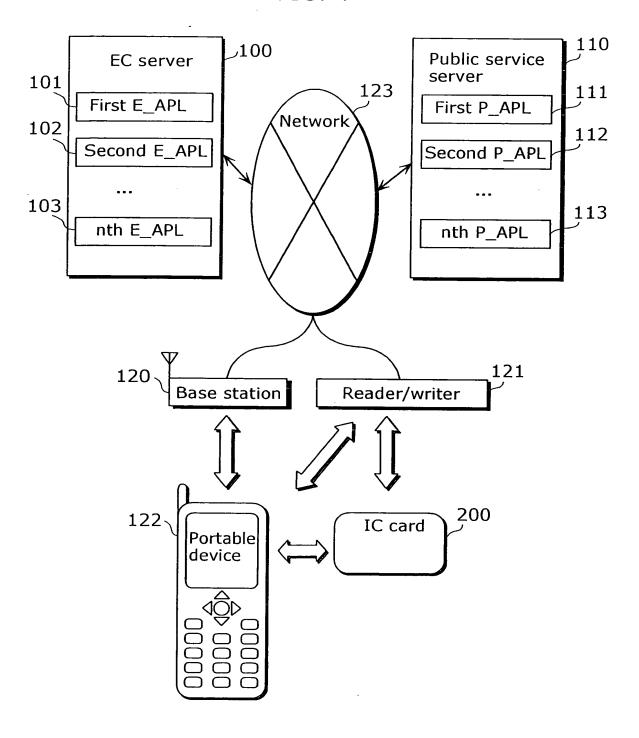


FIG. 5

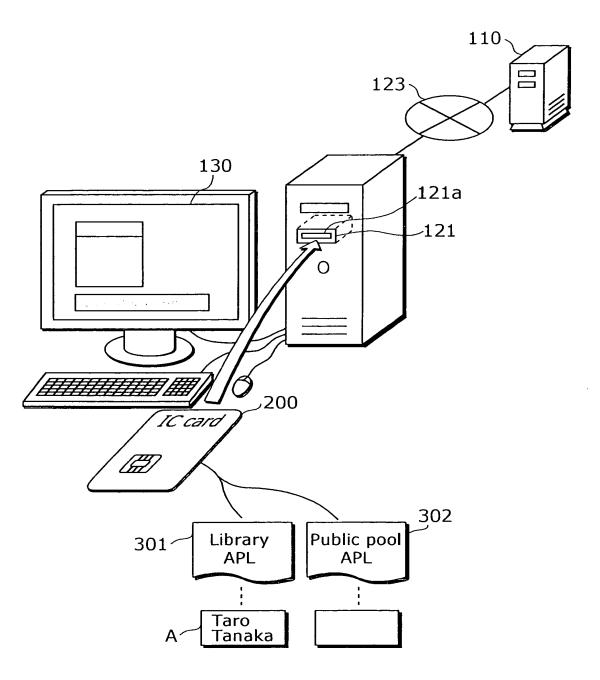
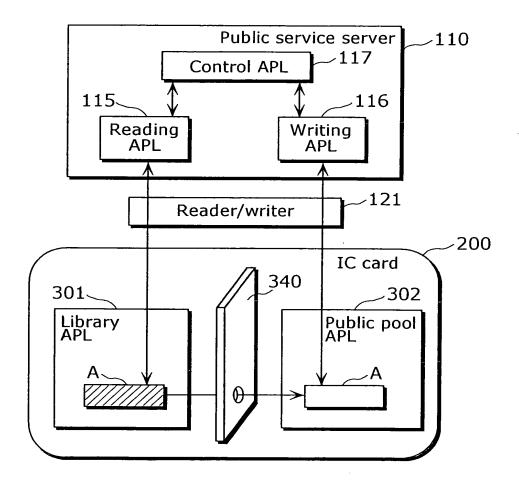


FIG. 6



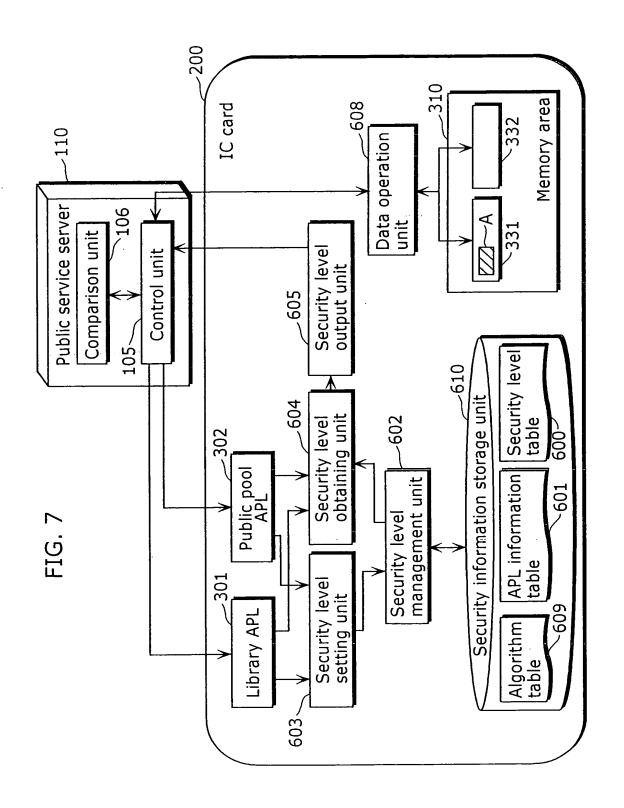


FIG. 8

	_	\sim	•
	h	1 1	•
_	v	v	•

Security level table						
Level Value Encryption algorithm						
Strong	03h	Triple-DES				
Medium	02h	DES				
Weak	01h	AES				
None	00h	No encryption				

FIG. 9

609

Algorithm table					
Number Encryption algorithm					
0	Triple-DES				
1	DES				
2	AES				
3	No encryption				

FIG. 10

	601						
APL information tab	APL information table						
	/						
Library APL information	1000	Application ID	2 bytes				
Public pool APL		Security level	2 bytes				
information		Encryption information	4 bytes				
•••		Key information	32 bytes				
Electronic money APL information		Protocol version information	4 bytes				

00h 00 Ph 00 0 00 00 00h 00h 00h 00h 90 P 00 0 00h 00 P : : : 00h 03h 90 P 90 Ph FDh 00 0 00h 33h 00h 02h 34h 00 00 02h 00h 78h 00 00 品 00h 22h 00h FFh 00h 00 Ph 00h 01h 12h 01h 80h 01h **56h** 03h S FFh 05h 11h FEh 03h S 1Ah Encryption information Encryption information Encryption information Version information Version information Version information Key information Key information Key information Application ID Application ID Application ID Security level Security level Security level Library APL information Public pool APL information Electronic money APL information FIG. 11

FIG. 12

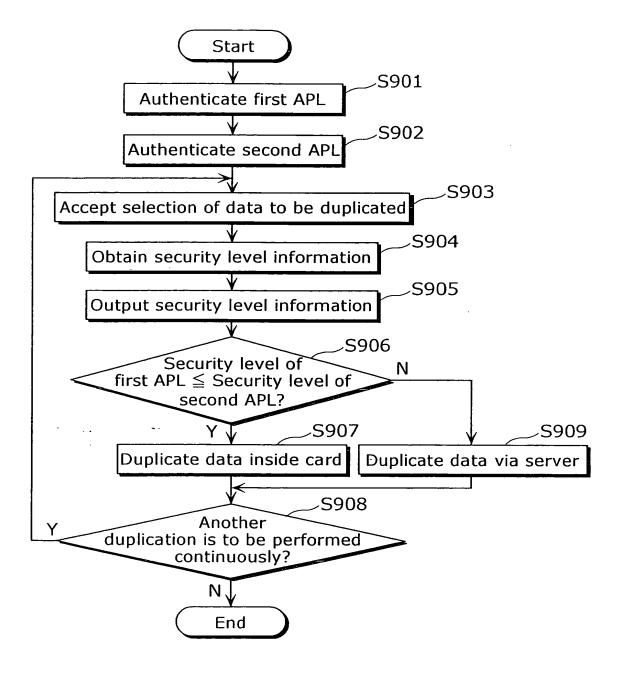
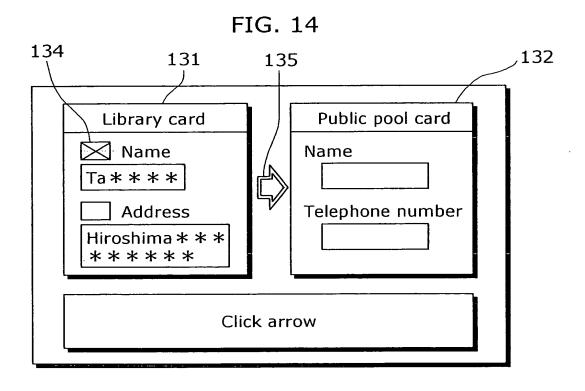


FIG. 13 130 132 131 Library card Select duplication destination Name -133Ta * * * * Public pool card **Address** Hiroshima * * * 00000 **** Duplicate data



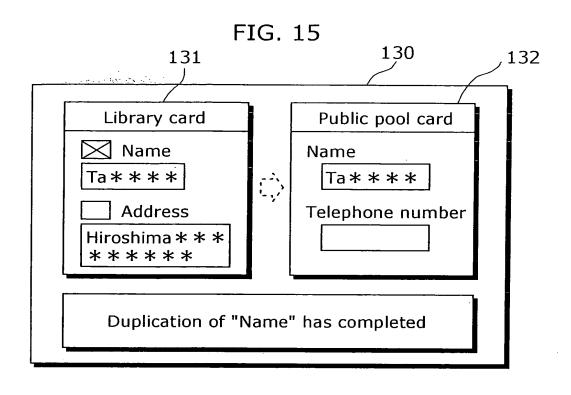
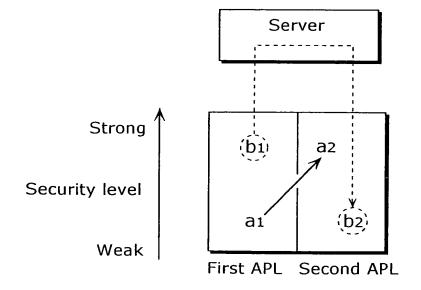
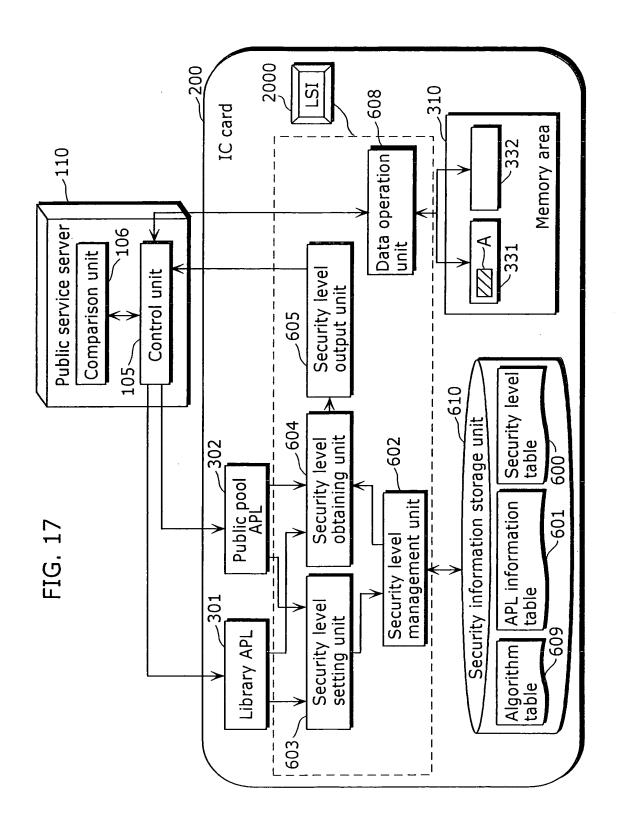


FIG. 16





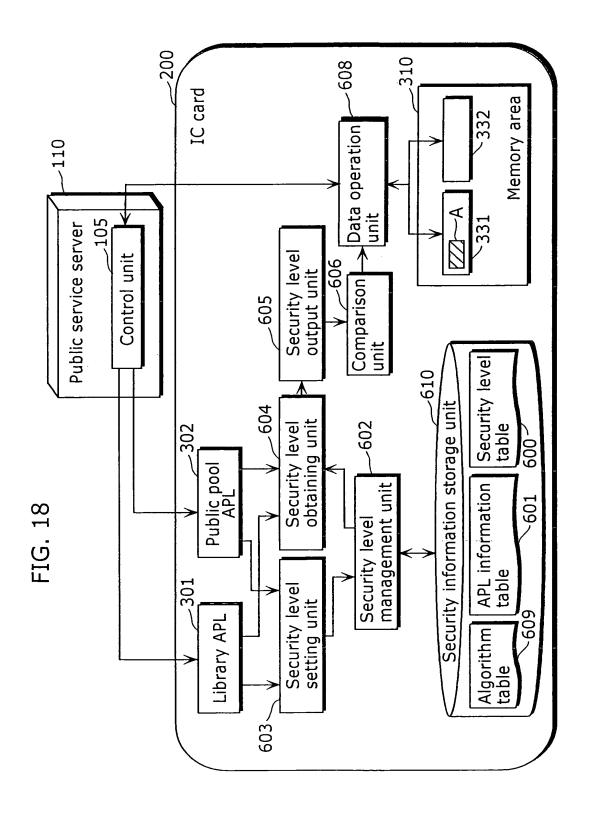
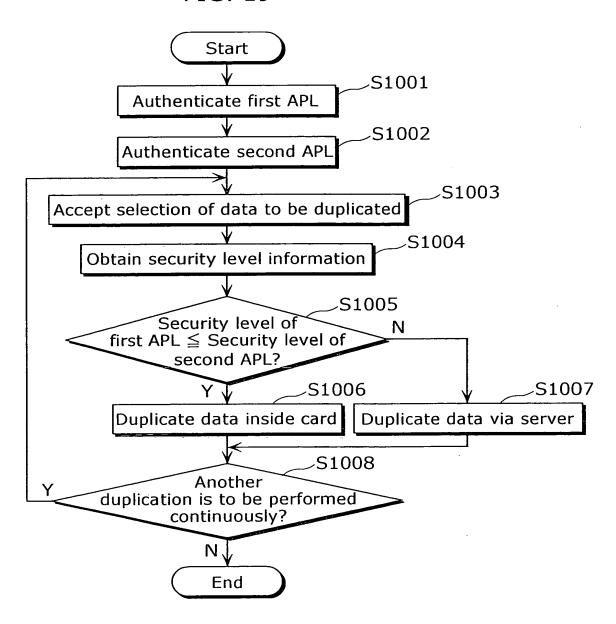


FIG. 19



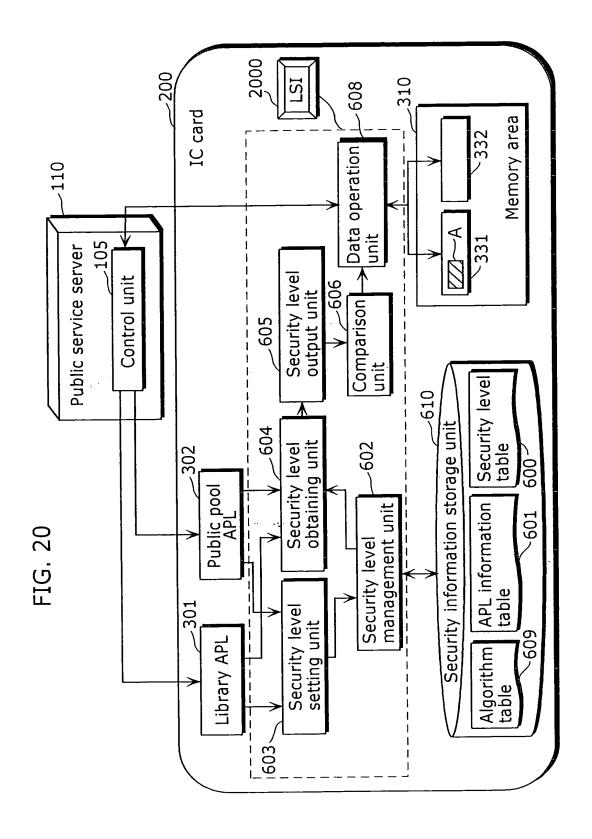


FIG. 21

CLA	INS	P1	P2	Lc	Data	Le
<ma< td=""><td>andato</td><th>ry head</th><th>der→</th><td>~</td><td>Conditional body</td><th><i>y</i>></th></ma<>	andato	ry head	der→	~	Conditional body	<i>y</i> >

FIG. 22

Command name	SELECT READ RECORD		INTERNAL AUTHENTICATE
CLA(1byte)	00h	00h	00h
INS(1byte)	A4h	B2	88h
P1(1byte)	XXh	Record Number	00h
P2(1byte)	00h	XXh	00h

FIG. 23

							_	
b8 b7 b6 b5 b4 b3 b2 b1 Meaning	Select MF, DF and EF	Select child DF	Select EF under current DF	Select parent DF of current DF	Direct selection by DF name	Select from MF	Select from current DF	Any other value: Not specified
b1	0	1	0	1	0	0	Ţ	
b2	0	0	1	Ţ	0	0	0	
b3	0	0	0	0	1	0	0	
b 4	0	0	0	0	0	1	+1	
p5	0	0	0	0	0	0	0	
9q	0	0	0	0	0	0	0	
b7	0	0	0	0	0	0	0	
p8	0	0	0	0	0	0	0	

FIG. 24

Data section	SW1	SW2
Body	Tra	iler→

FIG. 25

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0					Common command
1	0	0	0					Unique command

FIG. 26A **~200** IC card 202 201 205ر 203 .CPU IF**ROM** RAMFlash memory TRM area Secure 209 flash 206 208 **FeRAM** 207

FIG. 26B

